UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/693,378	10/23/2003	Chris D. Hyser	200205369-1	1637

22879 7590 12/19/2006

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
KOEMPEL THOMAS, BEATRICE L	
ART UNIT	PAPER NUMBER
2196	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/19/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/693,378	HYSER, CHRIS D.	
	Examiner	Art Unit	
	Bea Koempel-Thomas	2196	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *April 1, 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-18 are pending in this application and presented for examination.

Objections

Specification

2. The disclosure is objected to because of the following informalities:

3. Figures 1A-C are described as "one embodiment of the present invention," (page 1 lines 15-16 and page 3 lines 21-23), however they appear to be illustrating prior art.

4. Describing figure 2, page 5 lines 21 and 24 describe elements numbered 1904 and 1902, respectively. Figure 2 does not contain the cited reference numbers, but does show elements 204 and 202, which appear to represent the elements described. In order to further prosecution the examiner considered the elements as 204 and 202, respectively.

5. Reference characters "301" and "312," page 10, lines 8 and 20, respectively, have both been used to designate "the firmware module image." In order to further prosecution the examiner considered both references as 301, which appears to correspond to figure 3.

6. Reference character "306" has been used to designate both "an encrypted, hashed, module-specific public key" and "the next firmware module" (page 10 line 4 and page 11 line 19, respectively). In order to further prosecution the examiner considered 306 as referring to the element of the first reference, and 408 as referring to the element of the second reference; this appears to correspond to the elements included in the figures.

7. The disclosure contains an embedded hyperlink and/or other form of browser-executable code (page 9). Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

Appropriate correction is required.

Drawings

8. The formal drawings were received on April 1, 2004.

9. The drawings are objected to because: Figures 1A-C should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g).

10. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 202, 204, and 408. Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d).

11. Figure 3 is objected to for not corresponding to the disclosure regarding the flow from elements 303 to 306 as recited on page 10, lines 1-5 of the disclosure. This is pertinent to claims 3, and 7-9, which recite or depend from a claim that recites an "encrypted, hashed module-specific public key." Appropriate correction is required. Care should be taken that no new matter is added.

12. The drawings are objected to because: Figure 5 includes apparently extraneous lines appended to elements 308, 302, 301, and 314, which are not explained in the disclosure.

13. In addition to Replacement Sheets containing the corrected drawing figure(s), applicant is required to submit a marked-up copy of each Replacement Sheet including annotations indicating the changes made to the previous version. The marked-up copy must be clearly labeled as "Annotated Sheets" and must be presented in the amendment or remarks section that explains the change(s) to the drawings. See 37 CFR 1.121(d)(1). Failure to timely submit the proposed drawing and marked-up copy will result in the abandonment of the application.

14. Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will

be notified and informed of any required corrective action in the next Office action. The objections to the drawings will not be held in abeyance.

Claim Objections

15. Claims 2, 5, 6, 10, and 14-17 are objected to because of the following informalities (examiner interpreted grammar or spelling): claim 2 line 4 "describes" (describing); claims 5 and 14 lines 1-2 "method of" (deleted duplicate "method of"); claim 6 line 8 "module a value" (module with at value); claim 10 line 3 "module a value" (module with at value); claims 15-17 "an module" (a module). Appropriate correction is requested.

Claim Rejections - 35 USC § 101

16. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

17. Claims 5, 14-15 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

18. Claims 5 and 14 could reasonably be drawn to functional descriptive material, per se, i.e., "computer instructions" may be taken to mean software alone, and as such, claims 5 and 14 would be directed to non-statutory subject matter. The specification does not preclude this

interpretation. Further, claims 5 and 14 do not transform a physical object to a different state or thing nor produce a useful, concrete and tangible result.

19. Claim 15 is drawn to nonfunctional descriptive material, per se, i.e., "image of a module," which, just as a recorded photograph or motion picture, lacks functionality, thereby failing to satisfy the practical application requirement.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

20. Claims 1-7, and 14-18 are rejected under 35 U.S.C. 102(e) as being anticipated by Wyatt, U.S. Patent No. 7,007,159 B2 (hereinafter "Wyatt").

21. Regarding **claim 1:** Wyatt discloses a method for preparing an authenticable and verifiable image of a module, the method comprising:

receiving a module image (col. 7 lines 6-10);

adding to the module image a size (col. 8 line 39) and location (col. 8 lines 66) block (col. 9 lines 39-45);

adding to the module image an authentication block (col. 9 lines 63-64) including a cryptographically protected module-specific public key (col. 13 lines 14-15) and a clear-text version of the module-specific public key (col. 13 lines 14-16) to produce an authenticable image (col. 13 lines 17-25); and

adding to the authenticable image a verification block (col. 10 line 1) that includes a digital signature prepared from the module image (col. 12-13 lines 62-2).

22. Regarding **claim 2:** Wyatt discloses that adding to the module image a size and location block further includes:

adding, in a specific location (col. 9 lines 47-48), a header (col. 9 lines 39-45) that includes an image size (col. 8 line 39), location (col. 8 line 66), and globally unique identifier (col. 14 lines 30-31) describing a size and location of the firmware image (col. 14 lines 28-29) within a flash memory (col. 5 line 28) or other non-volatile memory (col. 5 line 27) and that identifies a class of machines for which the firmware module has been created (col. 14 line 28).

23. Regarding **claim 3:** Wyatt discloses that adding to the module image an authentication block including a cryptographically protected module-specific public key and a clear-text version of the module-specific public key to produce an authenticable image further includes:

adding to the module image an authentication block (col. 9 lines 63-64) including a hashed (col. 12 lines 65-67), encrypted module-specific public key (col. 13 lines 14-15) and a clear-text version of the module-specific public key (col. 13 line 5) to produce an authenticable image (col. 13 lines 17-25).

24. Regarding **claim 4:** Wyatt discloses that adding to the authenticable image a verification block that includes a digital signature prepared from the module image further includes:

adding to the authenticable image a verification block (col. 10 line 1) that includes a digital signature (col. 13 line 2) prepared by hashing the module image (col. 12-13 lines 67-1) and encrypting the hashed module image with a module-specific private key (col. 13 lines 1-2).

25. Regarding **claim 5:** Wyatt discloses computer instructions stored in a computer readable medium (col. 25 line 51).

26. Regarding **claim 6:** Wyatt discloses a method for authenticating and verifying an authenticable and verifiable module, the method comprising:

extracting, from the authenticable and verifiable module (col. 13 lines 11-16), a module-specific public key (col. 13 lines 14-15) and cryptographically protected data related to the module-specific public key (col. 14 lines 17-22);

comparing the cryptographically protected data (col. 14 lines 17-25) with the module-specific public key (col. 13 lines 14-15) to authenticate the authenticable and verifiable module;

comparing a value calculated from an image (col. 13 lines 26-28), including a size (col. 8 line 39) and location block (col. 8 line 66), included within the authenticable and verifiable module a value extracted from a digital signature (col. 12-13 lines 62-2) contained in a verification block within the authenticable and verifiable image to verify the authenticable and verifiable module (col. 13 lines 26-32).

27. Regarding **claim 7:** Wyatt discloses that extracting, from the authenticable and verifiable module, a module-specific public key and cryptographically protected data related to the module-specific public key further includes:

extracting, from an authentication block at a known location within the authenticable and verifiable image (col. 13 lines 11-12), a hashed (col. 12 lines 65-67), encrypted module-specific public key (col. 13 lines 14-15) and a clear-text version of the module-specific public key (col. 13 line 5).

28. Regarding **claim 14:** Wyatt discloses computer instructions stored in a computer readable medium (col. 25 line 51).

29. Regarding **claim 15:** Wyatt discloses an authenticable and verifiable image of an module stored in a computer-readable medium (col. 25 line 51) comprising:

a module image (col. 7 lines 6-10), including a size (col. 8 line 39), location (col. 8 line 66), and globally unique-identifier block (col. 14 lines 30-31);

an authentication block (col. 9 lines 63-64); and

a verification block (col. 10 line 1).

30. Regarding **claim 16:** Wyatt discloses an authentication block (col. 9 lines 63-64) containing a hashed (col. 12 lines 65-67), encrypted module-specific public key (col. 13 lines 14-15) and a clear-text version of the module-specific public key (col. 13 line 5) to produce an authenticable image (col. 13 lines 17-25).

31. Regarding **claim 17:** Wyatt discloses a verification block (col. 10 line 1) including a digital signature (col. 13 line 2) prepared by hashing the module image (col. 12-13 lines 67-1) and encrypting the hashed module image with a module-specific private key (col. 13 lines 1-2).

32. Regarding **claim 18:** Wyatt discloses a method for preparing an authenticable and verifiable image of a module, the method comprising:

a module-image receiving step (col. 7 lines 6-10);

a size-and-location-data adding step that adds size-(col. 8 line 39) and location (col. 8 lines 66) to the received module image (col. 7 lines 6-10);

an authentication-adding step that adds, to the module image, authentication information (col. 9 lines 63-64) including a cryptographically protected module-specific public key (col. 13 lines 14-15) and a clear-text version of the module-specific public key (col. 13 lines 14-16); and

a verification-block-adding step (col. 10 line 1) that adds a digital signature prepared from the module image to the module image (col. 12-13 lines 62-2).

Claim Rejections - 35 USC § 103

33. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

34. Claims 8-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wyatt in view of Thomlinson et al., U.S. Patent No. 6,272,631 B1 (hereinafter "Thomlinson").

35. Regarding **claim 8:** Wyatt discloses the clear-text version of the module-specific public key (col. 13 line 5); the hashed (col. 12 lines 65-67) encrypted module-specific public key (col. 13 lines 14-15) and a first private encryption key (col. 13 lines 1-2).

Wyatt does not disclose that comparing the cryptographically protected data with the module-specific public key to authenticate the authenticable and verifiable image further includes: hashing to produce a newly hashed key; decrypting; and comparing the decrypted, hashed key with the newly hashed key.

Thomlinson discloses that comparing the cryptographically protected data with the module-specific public key to authenticate the authenticable and verifiable image further includes: hashing to produce a newly hashed key (col. 8 lines 33-34); decrypting (col. 3 lines 40-41); and comparing the decrypted, hashed key with the newly hashed key (col. 8 lines 30-36).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wyatt with the multilevel key technique taught by Thomlinson in order to create a more secure architecture using "core" secrets during initialization.

36. Regarding **claim 9:** Wyatt discloses that when the decrypted, hashed module-specific public key is identical to the newly hashed module-specific public key, the authenticable and verifiable image is determined to be authenticated (col. 13 line 24).

37. Claims 10-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wyatt in view of Field et al., U.S. Patent No. 6,253,324 B1 (hereinafter "Field").

38. Regarding **claim 10:** Wyatt discloses a size (col. 8 line 39) and location (col. 8 line 66) block included within an authenticable and verifiable image (col. 9 lines 39-45); a verification block within the authenticable and verifiable image (col. 10 line 1), and a module-specific public key (col. 13 lines 17-25).

Wyatt does not disclose hashing an executable image to produce a newly hashed image; extracting a digital signature, and decrypting the digital signature to produce an extracted hashed image; and comparing the extracted hashed image to the newly hashed image.

Field discloses hashing an executable image to produce a newly hashed image (col. 9 lines 11-12); extracting a digital signature (col. 8 lines 27-28), and decrypting the digital signature (col. 8 lines 27-28) to produce an extracted hashed image (col. 8 line 29); and comparing the extracted hashed image to the newly hashed image (col. 9 lines 14-15).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wyatt with the multiple hashing technique taught by Field for the benefit of a more robust architecture securing sensitive information.

39. Regarding **claim 11:** Wyatt does not disclose that when the extracted hashed image is identical to the newly hashed image, the authenticable and verifiable image is determined to be verified.

Field discloses that when the extracted hashed image (col. 8 line 29) is identical to the newly hashed image (col. 9 lines 11-12), the authenticable and verifiable image is determined to be verified (col. 9 lines 16-19).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wyatt with the multiple hashing technique taught by Field for the benefit of a more robust architecture securing sensitive information.

40. Claims 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wyatt in view of Arbaugh et al., U.S. Patent No. 6,185,678 (hereinafter "Arbaugh").

41. Regarding **claim 12:** Wyatt discloses an authenticable and verifiable image (col. 9 lines 39-45); when the authenticable and verifiable image is authenticated and verified, the authenticable and verifiable image is accessed, executed, and/or incorporated (col. 13 lines 33-36), and when the authenticable and verifiable image is not authenticated or not verified, the authenticable and verifiable image is not executed and/or incorporated (col. 13 lines 33-36).

Wyatt does not disclose secure access, execution, and/or incorporation into a secure-computer processing environment.

Arbaugh discloses secure access, execution, and/or incorporation (col. 2 lines 59-60), into a secure-computer processing environment (col. 10 lines 53-56).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wyatt with the secure bootstrap architecture taught by Arbaugh to create a more secure robust computing platform.

42. Regarding **claim 13:** Wyatt discloses an authenticable and verifiable image (col. 13 lines 33-36), and an authenticable and verifiable image that is not executed and/or incorporated (col. 13 lines 33-36).

Wyatt does not disclose the method employed in the secure booting of a secure computer system, and failure of a secure boot.

Arbaugh discloses the method employed in the secure booting (col. 6 lines 6-7) of a secure computer system (Title), and failure of a secure boot (abstract lines 10-11 and col. 10 lines 13-14 and 24-25).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wyatt with the secure bootstrap architecture taught by Arbaugh to create a more secure robust computing platform.

Conclusion

Prior art made of record and not relied upon is considered pertinent to applicant's disclosure is:

- "Secure Hash Standard," Federal Information Processing Standards Publication 180-1, April 17, 1995.
- Worley, Jr. et al., U.S. Patent No. 7,073,059 B2, regarding a secure machine platform that interfaces to operating systems and customized control programs.
- Fish et al., U.S. Patent No. 6,401,201 B2, regarding firmware support.
- Fish et al., U.S. Patent No. 6,381,693 B2, regarding firmware support.
- Byers et al., U.S. Patent No. 6,959,184 B1, regarding a method for determining security status.
- Sprunk et al., U.S. Patent No. 5,754,659, regarding generation of cryptographic signatures using hash keys.
- Iwamura, U.S. Patent No. 6,425,081 B1, regarding an electronic watermark system.

- Hawkes et al., U.S. Patent Publication No. 2004/0019785 A1, regarding efficient encryption and authentication.

Please direct any inquiry concerning this communication or earlier communications from the examiner to Bea Koempel-Thomas whose telephone number is 571-270-1252. The examiner can normally be reached on Monday - Thursday & alternate Fridays; 0730 - 1700.

If attempts to reach the examiner by telephone are unsuccessful, please contact the examiner's supervisor, Nabil El-Hady, on 571-272-3963. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

bkt 12/11/2006

NABIL M. EL-HADY
SUPERVISORY PATENT EXAMINER